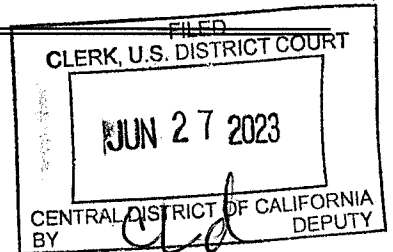


UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of)

(Briefly describe the property to be searched or identify the
person by name and address))A white, 2015 Volkswagen Jetta, bearing California
license plate 7LVM035, and Vehicle Identification
Number ("VIN") 3VWD17AJ7FM407444. *SDL* *[initials]*

Case No. 2:23-mj-03230-DUTY

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-2

located in the Central District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841(a)(1)	Possession with Intent to Distribute Controlled Substances
21 U.S.C. § 846	Conspiracy
18 U.S.C. § 924(c)	Carrying a firearm during and in relation to, and possessing a firearm in furtherance of, a drug trafficking crime
18 U.S.C. § 922(g)	Prohibited person in possession of a firearm

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Sean D. Lusk, Task Force Officer

Applicant's signature

Sean D. Lusk, TFO, FBI Central Coast Safe Streets Task Force
Officer, CHP- Coastal Division

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 6/27/2023City and state: Los Angeles, CA

AUSA: Alix McKenna x6166

Judge's signature

Hon. Jacqueline Chooljian, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A-2

VEHICLE TO BE SEARCHED

32. A white, 2015 Volkswagen Jetta, bearing California license plate 7LVM035, and Vehicle Identification Number ("VIN") 3VWD17AJ7FM407444~~8~~, (the "SUBJECT VEHICLE").

SOL
by [signature]

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) (possession with intent to distribute controlled substances) and 846 (conspiracy), and 18 U.S.C. §§ 922(g) (prohibited person in possession of a firearm) and 924(c) (carrying a firearm during and in relation to, and possessing a firearm in furtherance of, a drug trafficking crime) (the "Subject Offenses"), namely:

a. All firearms and ammunition, and firearm parts or accessories, including but not limited to shell casings, magazine clips, silencers, scopes, and ammunition boxes.

b. Items pertaining to the possession and/or manufacturing of firearms, including but not limited to gun cases, ammunition magazines, unfinished lower receivers, hand guards, rifle barrels, holsters, spare parts for firearms, firearms cleaning equipment, drills, drill bits, tools, vises, and receipts for the purchase and/or repair of these items.

c. All documents or devices noting the price, quantity, dates, and/or times when firearms were purchased, possessed, transferred, distributed, or sold, including but not limited to firearms money ledgers, firearms distribution or customer lists, price lists, firearms supplier lists, maps and written directions to locations, correspondence, notation logs, receipts, journals, books, pay and owe sheets, telephone

records, telephone bills, address books, bank statements, storage unit receipts, and wire transfer receipts.

d. All records or documents related to or establishing the identities of co-conspirators, customers, and third-party sources of weapons.

e. Any controlled substance, controlled substance analogue, or listed chemical;

f. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;

g. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

h. United States currency over \$1,000 or bearer instruments worth over \$1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first \$1,000), and data, records, documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or transferring money over \$1,000, such as bank account records, cryptocurrency records and accounts;

i. Documents and records reflecting the identity of,

contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances or firearms, or drug or firearms customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs, guns, or ammunition, were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

j. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

k. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

l. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written

communications sent to or received from any digital device and which relate to the above-named violations;

m. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs, guns, or ammunition were bought, sold, or otherwise distributed;

n. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs, guns, or ammunition;

o. Contents of any calendar or date book;

p. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

q. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

r. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR THE SUBJECT DEVICES

1. In searching the SUBJECT DEVICES (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICES as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital devices and/or forensic images thereof beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK"

(Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been

able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICES, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

2. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

3. During the execution of this search warrant, law enforcement is permitted to (1) depress VILLAREAL's thumb- and/or fingers onto the fingerprint sensor of the SUBJECT DEVICES (only if the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of VILLAREAL's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may

use no more than objectively reasonable force in light of the facts and circumstances confronting them.

4. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Sean D. Lusk, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Task Force Officer ("TFO") with the FBI assigned to the Central Coast Safe Streets Task Force. I am also employed as a full-time, sworn law enforcement officer for the California Highway Patrol ("CHP") and have been for the past 23 years. I am currently assigned to the Coastal Division Investigative Services Unit. My primary responsibility is to investigate and assist other officers and allied agencies with in-depth investigations involving criminal street gangs, weapons, and narcotics violations.

2. I attended and graduated from the California Highway Patrol Academy and hold Basic, Intermediate, and Advanced Certificates from California Peace Officer Standards and Training. I have completed a 72-hour Drug Recognition Expert course certified by the International Association of Chiefs of Police and over 80 hours of narcotics and criminal interdictions training relating to the transportation, concealment, trends, and sales of illegal narcotics and other criminal activities. I have spoken on numerous occasions with other officers and experts in the field of narcotics interdiction regarding current trends on narcotic sales and trafficking.

3. As a TFO, I have participated in numerous investigations involving federal firearm and drug offenses and participated in the execution of numerous arrest and search warrants. I have also participated in the interviews of

defendants, informants, and witnesses who had personal knowledge of firearm and drug trafficking methods.

II. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrant for Gilbert Noel Villareal ("VILLAREAL") for a violation of 21 U.S.C. §§ 841(a)(1), (b)(1)(A)(viii) (possession with intent to distribute methamphetamine).

2. This affidavit is also made in support of a search warrant for the following digital devices (collectively, the "SUBJECT DEVICES"), in the custody of the CHP in San Luis Obispo, California, as described more fully in attachment A-1:

a. A black Motorola G-Pure cellular phone with an IMEI of 358385282111601, seized on June 16, 2023, from the person of VILLAREAL ("SUBJECT DEVICE 1");

b. A black Apple iPhone cellular phone of an unknown model, with an IMEI of 353814087489842, seized on June 16, 2023, from the center console of the SUBJECT VEHICLE ("SUBJECT DEVICE 2");

c. A black Samsung Galaxy Z Fold cellular phone, with an IMEI of 356254950548738, seized on June 16, 2023, from the center console of the SUBJECT VEHICLE ("SUBJECT DEVICE 3");

d. A black Microsoft Laptop of an unknown model, with a serial number of 022754173253, seized on June 16, 2023, from the trunk area of the SUBJECT VEHICLE ("SUBJECT DEVICE 4").

3. This affidavit is also made in support of applications for warrants to search the following:

a. A white, 2015 Volkswagen Jetta, bearing California license plate 7LVM035, and Vehicle Identification Number ("VIN") 3VWD17AJ7FM407444, as described more fully in Attachment A-2 (the "SUBJECT VEHICLE"); and

b. The person of VILLAREAL, as described more fully in Attachment A-3.

4. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) (possession with intent to distribute controlled substances) and 846 (conspiracy), and 18 U.S.C. §§ 922(g) (prohibited person in possession of a firearm) and 924(c) (carrying a firearm during and in relation to, and possessing a firearm in furtherance of, a drug trafficking crime) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A-1, A-2, A-3, and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only and all dates and times are on or about those indicated.

III. SUMMARY OF PROBABLE CAUSE

6. On June 16, 2023, at approximately 7:40 p.m., California Highway Patrol ("CHP") Officer Toby Hall conducted a traffic stop on a white 2015 Volkswagen Jetta (the "SUBJECT VEHICLE") driven by Gilbert Noel VILLAREAL on Harris Grade Road, in the County of Santa Barbara. VILLAREAL --- the sole occupant --- falsely identified himself to Officer Hall by providing a counterfeit U.S. Permanent Resident Card bearing the name of "A.N." VILLAREAL told OFFICER HALL that he did not have a driver license. Officer Hall noted that the identification card provided by VILLAREAL was flimsy and delaminating which, based on his training and experience, led Officer Hall to question the validity of the identification.

7. Officer Hall returned to his patrol vehicle and conducted a driver license check. He did not find a match using the name and date of birth provided by VILLAREAL but found numerous warrants for individuals using that name with similar descriptions.

8. Officer Hall directed VILLAREAL to exit the SUBJECT VEHICLE and performed a search of his person for further identification. He placed him in handcuffs and removed SUBJECT DEVICE 1 from VILLAREAL's hand. During a pat down, Officer Hall recovered a switchblade knife with a retractable blade in VILLAREAL's left front pants pocket, in violation of California Penal Code Section 21510.

9. A search of VILLAREAL's wallet revealed a California Driver License and California Identification Card identifying

VILLAREAL's true identity, and a fake Social Security Card in the name of "A.N.". Officer Hall placed VILLAREAL under arrest for several offenses, including false identification to a peace officer, possession of a switchblade, and possession of a counterfeit seal, and requested a tow truck for the SUBJECT VEHICLE.

10. Officer Hall began an inventory search of the SUBJECT VEHICLE. During the inventory search, Officer Hall located SUBJECT DEVICES 2 through 4, approximately 20.5 grams of suspected fentanyl, approximately 645.8 grams of suspected methamphetamine, drug use paraphernalia, several digital scales, and small baggies often utilized for packaging narcotics.

IV. STATEMENT OF PROBABLE CAUSE

11. Based on my review of law enforcement reports, conversations with other law enforcement agents, my review of a video recording of VILLAREAL's traffic stop and arrest, and my own knowledge of the investigation, I am aware of the following:

A. CHP Officer Hall conducted a traffic stop on the SUBJECT VEHICLE.

12. On June 16, 2023, at approximately 7:40 p.m., while on patrol, CHP Officer Hall was parked facing southbound on the right shoulder of Harris Grade Road north of Burton Mesa Boulevard, when Officer Hall saw the SUBJECT VEHICLE traveling southbound. As it passed his location, he noted the side windows were darkly tinted and the driver began to roll down the side windows. Officer Hall pulled up behind the SUBJECT VEHICLE and conducted a traffic stop.

13. Officer Hall contacted the sole occupant of the SUBJECT VEHICLE, later identified as VILLAREAL. VILLAREAL related to Officer Hall that he did not have a driver license and stated he only had his "green card". VILLAREAL then provided Officer Hall with what purported to be a United States of America Permanent Resident Card from his wallet. Officer Hall also noted VILLAREAL's wallet was bulging with money and observed several other cards in the wallet, including what appeared to possibly be a California Driver License or Identification Card. Officer Hall was unable to confirm the additional potential identification cards because VILLAREAL quickly closed his wallet.

14. The purported resident identification card contained an image of VILLAREAL but displayed the name "A.N." According to Officer Hall, the card appeared to possibly be fraudulent because it was flimsy and delaminated. Officer Hall later related to me that he has seen numerous real and fraudulent resident identification cards and believed that the one VILLAREAL provided may have been fraudulent.

15. Officer Hall returned to his patrol vehicle and conducted a wants and warrants check for "A.N." Officer Hall was unable to locate a match with the name and date of birth listed on the resident identification card. Officer Hall did locate several warrants for the name on the resident identification card with similar descriptors. Officer Hall returned to the SUBJECT VEHICLE and directed VILLAREAL to exit, and VILLAREAL complied.

16. Due to VILLAREAL's inability to provide satisfactory identification, Officer Hall detained VILLAREAL. Officer Hall removed a wallet and SUBJECT DEVICE 1 from VILLAREAL's hand, handcuffed him, and placed him inside the patrol vehicle. Officer Hall also located a knife with a retractable blade in VILLAREAL's left front pants pocket. The knife appeared to constitute a switchblade, the possession of which is restricted under California Penal Code Section 21510.

B. Officer Hall located identification with VILLAREAL's true identity and arrested VILLAREAL.

17. After placing VILLAREAL into the patrol vehicle, Officer Hall opened VILLAREAL's wallet and located a California Driver's License, and a California Identification Card, both bearing VILLAREAL's true name and identifying information, along with a fake social security card bearing the name "A.N.".

18. Officer Hall placed VILLAREAL under arrest for several charges, including false identification to a peace officer, possession of a switchblade, and possession of a counterfeit seal.

C. Officer Hall requested a tow truck and conducted an inventory search of the SUBJECT VEHICLE.

19. Officer Hall requested a tow truck for the SUBJECT VEHICLE. Officer Hall also learned that VILLAREAL had a valid driver license under his true name and had two outstanding warrants in Santa Barbara County. One warrant was for a violation of the terms of postrelease community supervision, under California Penal Code section 3455(b)(1); Transportation/Importation/Sale/Furnishing/Giving Away a

Controlled Substance, in violation of California Health and Safety Code section 11379(a); and Felon with a Firearm, in violation of Penal Code section 29800(a)(1). The second warrant was for Possession for Sale of a Controlled Substance, in violation of California Health & Safety Code Section 11378; Transportation/Importation/Sale/Furnishing/Giving Away a Controlled Substance, in violation of California Health and Safety Code section 11379(a); and Possession of Controlled Substances while Armed, in violation of Health and Safety Code section 11370.1.

20. Officer Hall began to inventory the SUBJECT VEHICLE and located SUBJECT DEVICE's 2 and 3 in the center console and SUBJECT DEVICE 4 in a backpack in the trunk. Officer Hall also located several digital scales, several pipes and syringes, approximately 20.5 grams of suspected fentanyl, approximately 645.8 grams of suspected methamphetamine, numerous plastic bags of varying sizes, and approximately \$2,243 in US currency recovered from VILLAREAL's wallet and the center console of the SUBJECT VEHICLE.

D. Officer Hall transported VILLAREAL to the CHP Office for evidence processing and interview.

21. Officer Hall completed the storage records for the SUBJECT VEHICLE and transported VILLAREAL to the CHP Buellton Area Office. Upon his arrival, he read VILLAREAL his Miranda rights in the presence of CHP Sergeant Fajardo, who was present during the interview. VILLAREAL agreed to speak with the Officers and claimed ownership of the contents of the SUBJECT

VEHICLE. VILLAREAL admitted to the officers that he sold drugs to support both his habit and his family. VILLAREAL identified the seized drugs as methamphetamine and fentanyl. He also identified the pipes and syringes as items he carried so people could use drugs when they purchased from him. He also admitted he had been arrested numerous times for possession and possession for sales.

E. The FBI obtains the suspected methamphetamine and fentanyl from the CHP.

22. On or about June 22, 2023, I obtained the seized suspected methamphetamine and fentanyl. The evidence items, including the suspected methamphetamine and fentanyl were processed and booked into FBI custody. On the same day, I sent the suspected methamphetamine and fentanyl to the DEA Southwest Laboratory for testing. Prior to being shipped, I performed a presumptive test on two packages recovered from the SUBJECT VEHICLE containing suspected methamphetamine. Both tests were positive for methamphetamine.

F. VILLAREAL further incriminates himself in recorded jail calls

23. Based on my review of jail calls from Santa Barbara County Jail, VILLAREAL made the following admissions:

a. On or about June 16, 2023, at approximately 11:31 p.m., VILLAREAL called phone number ending in 0830, identified in the jail call system as being associated with M.T. During the call, VILLAREAL told M.T. that he called another female, L.C., when he got pulled over and told her that if the cops asked, she should tell them his name was "Anthony Nunez." In response to

M.T.'s question about whether police got anything on VILLAREAL, VILLAREAL stated yes and indicated he had a gun (a "strap"), drugs, and a fake identification.

b. On or about June 17, 2023, at approximately 12:04 a.m., VILLAREAL called M.T. again. They talked about VILLAREAL calling someone when he got stopped. Based on the context of their conversation, I believe that they were referring to L.C. VILLAREAL told M.T. he told the cop he just bought this vehicle, and the cops could talk to the owner. M.T. asked about why police stopped VILLAREAL. In response, he stated it was for tinted windows, and M.T. responded something to the effect, "I told you babe." He stated I regret even buying that car. VILLAREAL stated that he thought about running from the police during the traffic stop.

c. On or about June 17, 2023, at approximately 10:48 a.m., VILLAREAL called M.T. again. During the call, VILLAREAL related that he sells drugs but, also uses and cannot stop using.

G. Information obtained regarding the SUBJECT VEHICLE.

24. On or about June 26, 2023, I obtained a California DMV registration print for the SUBJECT VEHICLE. The registration indicated that the registered owner of the SUBJECT VEHICLE was L.C. at an address in Lompoc, California. The printout also indicated a release of liability with a receipt date of June 23, 2023, with a transfer date of June 15, 2023, to M.T. at an address in Lompoc.

25. AS discussed above, I know based on my review of jail calls, VILLAREAL made numerous calls to a person indicated on the Santa Barbara County Jail phone record system as being associated with M.T.

H. VILLAREAL is a convicted felon

26. VILLAREAL has been convicted of multiple felonies, including the following:

a. On September 10, 2002, VILLAREAL was sentenced to 16 months in California State Prison for a felony charge of Possession for Sale of a Controlled Substance, in violation of California Health & Safety Code Section 11378.

b. On July 11, 2006, VILLAREAL was sentenced to 6 years in California State Prison for a felony charge of Transportation/Importation/Sale/Furnishing/Giving Away a Controlled Substance, in violation of California Health & Safety Code Section 11379(a).

c. On April 15, 2010, VILLAREAL was sentenced to 3 years in California State Prison for a felony charge of Evading a Peace Officer, in violation of California Vehicle Code section 2800.2(a).

d. On June 15, 2011, VILLAREAL was sentenced to 2 years in California State Prison for a felony charge of Dissuading a Witness in violation of Penal Code section 136.1(c)(1).

e. On April 19, 2016, VILLAREAL was sentenced to fifteen years in California State Prison after being convicted of felony charges of Felon in Possession of a Firearm, in

violation of California Penal Code section 29800(a)(1), and Transportation/Importation/Sale/Furnishing/Giving Away a Controlled Substance, in violation of California Health and Safety Code section 11379(a).

I. Surveillance conducted for VILLAREAL.

27. On or about June 26, 2023, I learned that VILLAREAL was released from the Santa Barbara County Jail after posting bond. I had also previously learned from FBI TFO Justin Francis that the SUBJECT VEHICLE had been released from the tow yard. TFO Francis learned from the tow company that the SUBJECT VEHICLE was released to the registered owner, L.C., by the tow company. I am unsure if the release of liability was on file when the June 16, 2023 arrest occurred.

28. On June 26, 2023, at approximately 1:30 p.m., I located the SUBJECT VEHICLE parked in the Motel 6 parking lot on North H Street in Lompoc, California. At approximately 2:00 p.m., VILLAREAL was identified by investigators standing in the doorway of Room 218 at the Motel 6. Another male with a bicycle was observed standing outside of room 218. A short time later, a shorter Hispanic female was observed exiting Room 218 before reentering the room. The male on the bicycle left, and VILLAREAL went back inside Room 218 and the door closed. I also noted the SUBJECT VEHICLE was parked just below and to the west of the Room 218.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

29. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, in vehicles they use, and/or at the places they reside. Drug traffickers also often keep drugs, drug packaging, scales, and cash in places that are readily accessible to them, and under their physical control, such as in their vehicles and/or places they reside.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the

seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residence, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their narcotics and may keep stashes of narcotics in their vehicles in the event of an unexpected opportunity to sell narcotics arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence, in their vehicles, or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital scales, packaging materials, and

proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

VI. TRAINING AND EXPERIENCE ON FIREARM OFFENSES

30. From my training, personal experience, and the collective experiences related to me by other law enforcement officers who conduct who conduct firearms investigations, I am aware of the following:

a. Persons who possess, purchase, or sell firearms generally maintain records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such as, in their vehicles or in their digital devices. It has been my experience that prohibited individuals who own firearms illegally will keep the contact information of the individual who is supplying firearms to prohibited individuals or other individuals involved in criminal activities for future

purchases or referrals. Such information is also kept on digital devices.

b. Many people also keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices. These photographs and recordings are often shared via social media, text messages, and over text messaging applications.

c. Those who illegally possess firearms often sell their firearms and purchase firearms. Correspondence between persons buying and selling firearms often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price. In my experience, individuals who engage in street sales of firearms frequently use phone calls, e-mail, and text messages to communicate with each other regarding firearms that they sell or offer for sale. In addition, it is common for individuals engaging in the unlawful sale of firearms to have photographs of firearms they or other individuals working with them possess on their cellular phones and other digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms.

d. Individuals engaged in the illegal purchase or sale of firearms and other contraband often use multiple digital devices.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

19. As used herein, the term "digital device" includes the SUBJECT DEVICES.

20. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable

data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

21. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which

may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

22. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the

opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress VILLAREAL's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of VILLAREAL's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

VIII. CONCLUSION

31. For all the reasons described above, there is probable cause to believe that VILLAREAL violated 21 U.S.C. §§ 841(a)(1), (b)(1)(A)(viii) (possession with intent to distribute methamphetamine). Further, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offense, will be found on the SUBJECT DEVICES, as described in Attachment A-1, the SUBJECT VEHICLE, as described in Attachment A-2, and on VILLAREAL's person, as described in Attachment A-3.

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this 27th day of
June, 2023.



HONORABLE JACQUELINE CHOOLJIAN
UNITED STATES MAGISTRATE JUDGE